DOMANDE QUANTUM

Domande esami vecchi (in giallo domande esami molto vecchi)

1. **Si definisca cosa è un qubit e come viene rappresentato lo stato di un qubit ai fini dell'elaborazione quantistica.**

   Un qubit (Quantum-bit) è un'entità logica che rappresenta l'informazione quantistica, viene trattato come un oggetto matematico.

   Il suo vector state è rappresentato da $|\psi> = \alpha|0> + \beta|1>$ con |0> =$\begin{pmatrix}1\\0\end{pmatrix}$ ed |1> =$\begin{pmatrix}0\\1\end{pmatrix}$.

   Alpha e beta sono le probability amplitudes: quando un qubit viene misurato si ottiene 0 oppure 1 con probabilità alpha^2 o beta^2. Lo state vector di un qubit può essere rappresentato convenzionalmente su una bloch sphere

   $$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

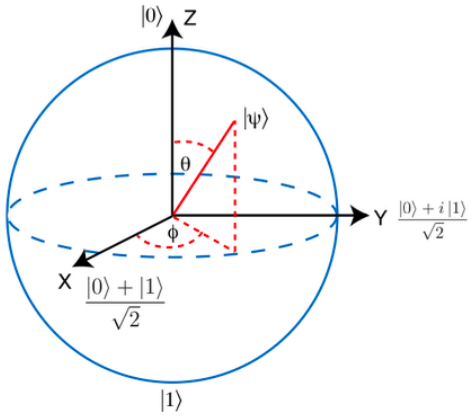
   

   Figure 1: The state of a qubit, represented on the Bloch sphere.

2. **Si illustrino i postulati della meccanica quantistica.**
   1. Qualsiasi sistema fisico isolato ha uno spazio vettoriale di dimensione finita con un inner product, noto come state space del sistema (poter sostituire con Spazio di Hilbert). Il sistema è descritto completamente da un vettore di stato, che è un vettore unitario nello spazio di stato del sistema.
   2. L'evoluzione temporale di un sistema quantistico chiuso è descritta dalla trasformazione unitaria |ψ'>=U|ψ> dove |ψ> è lo stato del sistema al tempo t_1 e |ψ'> è quello al tempo t_2, U è l'operatore unitario che dipende solo da t_1 e t_2.
   3. Una misurazione quantistica è descritta da un operatore Hermitiano M che ha la seguente decomposizione spettrale: $M = \sum_m mP_m$ dove P_m = |m><m| è il proiettore sull'eigenspace di M associato all'autovalore $m \in \mathbb{R}$
   4. Lo spazio di stato di un sistema fisico composito è il prodotto tensoriale degli spazi di stato dei sistemi fisici componenti. Se abbiamo n sistemi preparati negli stati {|ψ_i>, …, |ψ_n>}, lo stato congiunto del sistema totale è: |ψ_1>⊗ |ψ_2>⊗ … ⊗ |ψ_n>

3. **Si spieghi il concetto di stato quantistico *entangled*, portando qualche esempio. Si illustri il circuito quantistico per generare gli stati di Bell.**

   Gli entangled states sono gli stati non decomponibili in tensor product di stati componenti (non rispettano il quarto postulato). I loro risultati di misurazione sono correlati, un esempio sono i Bell states (basi di $\mathbb{C}^4$):

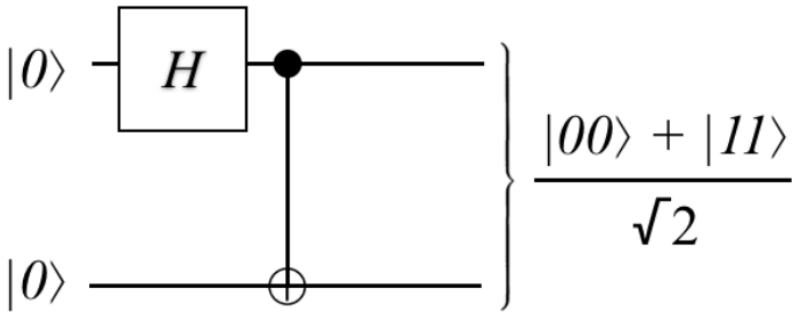
   $$|\beta_{00}| = \frac{|00> + |11>}{\sqrt{2}}$$

   $$|\beta_{01}| = \frac{|01> + |10>}{\sqrt{2}}$$

   $$|\beta_{10}| = \frac{|00> - |11>}{\sqrt{2}}$$

   $$|\beta_{11}| = \frac{|01> - |10>}{\sqrt{2}}$$

   Il circuito per generare uno stato di Bell è il seguente:



4. **Si illustrino i postulati della meccanica quantistica in termini delle matrici densità.**

   Uno stato misto è un insieme statistico di diversi stati quantistici $|\psi_i>$, con rispettive probabilità p_i.

   1. Un sistema quantistico che si trova in un mixed state è completamente descritto da un operatore di densità, definito dalla seguente equazione:

      $$\boldsymbol{\rho} = \sum p_i |\psi_i >< \psi_i|$$

      Deve soddisfare due condizioni: essere *definito semi-positivo*, e avere $tr(\rho) = 1$

2. Se un sistema quantistico si evolve in un nuovo stato U$|\psi_i>$ dove U è l'operatore unitario, l'operatore densità risultante è:

$$\sum_i p_i U|\psi_i><\psi_i|U^\dagger = U\rho U^\dagger$$

3. Se si esegue una misurazione descritta dal proiettore $\{P_m\}$, la probabilità di ottenere un risultato m è: $p(m) = \sum_i p(m|i)p_i = tr(\rho P_m)$
4. La rappresentazione della matrice di un operatore di densità è chiamata matrice densità, un sistema composto ha matrice densità:

$$\boldsymbol{\rho_{AB}} = \sum_{\boldsymbol{ijkl}} \boldsymbol{c_{ijkl}}|\boldsymbol{a_i}><\boldsymbol{a_j}| \otimes |\boldsymbol{b_k}><\boldsymbol{b_l}|$$

Con $\{|\boldsymbol{a_i}>\}$ che rappresenta l'Hilbert space di V_A e $\{|\boldsymbol{b_i}>\}$ l'Hilbert space V_B

E' possibile ricavare la matrice densità ridotta per il subsystem A prendendo la traccia parziale su B.

$$\rho_A = tr_B(\rho_{AB}) = \sum_{ijkl} c_{ijkl}|\boldsymbol{a_i}><\boldsymbol{a_j}| < \boldsymbol{b_l}|\boldsymbol{b_k}>$$

5. Si illustri il concetto di quantum fidelity.

La quantum fidelity è una misura di distanza quantistica, permette di stabilire quanto siano vicini due quantum state tra loro. Supponiamo di avere due density operators (ρ, σ), la Fidelity è definita come:

$F(\rho,\sigma) = (tr\sqrt{\sqrt{\rho\sigma}\sqrt{\rho}})^2$

Se solo ρ è puro si ha: $F(\rho,\sigma) = <\psi|\ \sigma\ |\psi>$

Se entrambi gli stati sono puri, allora $F(\rho,\sigma) = |<\psi|\theta>|^2$

6. Si presentino i principali operatori quantistici a singolo qubit.

Gli operatori agiscono su più qubits, e sono descritti da matrici unitarie U in modo che $UU^\dagger = I$ -> i quantum gates sono *reversibili*, è sempre possibile invertire un quantum gate con un altro quantum gate. Ciò significa che, dato l'output di un quantum gate, è sempre possibile determinare quale fosse l'input.
I gate principali a singolo qubit sono:

a. **Hadamard gate, H =** $\frac{1}{\sqrt{2}}\begin{pmatrix}\boldsymbol{1} & \boldsymbol{1}\\ \boldsymbol{1} & \boldsymbol{-1}\end{pmatrix}$, corrisponde ad una rotazione di pi/2 sull'asse delle y, seguito da una riflessione del piano x-y sulla bloch sphere.
b. **Pauli-X, X =** $\begin{pmatrix}\boldsymbol{0} & \boldsymbol{1}\\ \boldsymbol{1} & \boldsymbol{0}\end{pmatrix}$, corrisponde ad una rotazione di pi sull'asse x, è l'equivalente quantistico del classico NOT gate.
c. **Pauli-Y, Y =** $\begin{pmatrix}\boldsymbol{0} & \boldsymbol{-i}\\ \boldsymbol{i} & \boldsymbol{0}\end{pmatrix}$, corrisponde ad una rotazione di pi sull'asse y.
d. **Pauli-Z, Z =** $\begin{pmatrix}\boldsymbol{1} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{-1}\end{pmatrix}$, corrisponde ad una rotazione di pi sull'asse z.

e. **Phase, S =** $\begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{i} \end{pmatrix}$

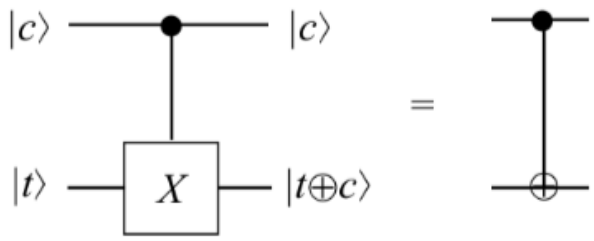
f. $\boldsymbol{\pi/8}$**, T =** $\begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{e^{i\frac{\pi}{4}}} \end{pmatrix}$

g. **Phase shift,** $\mathbf{R_\phi}$**=** $\begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{e^{i\phi}} \end{pmatrix}$

h. **Square-root-of-NOT,** $\sqrt{\mathbf{NOT}}$ **=** $\frac{\mathbf{1}}{\mathbf{2}}\begin{pmatrix} \mathbf{1+i} & \mathbf{1-i} \\ \mathbf{1-i} & \mathbf{1+i} \end{pmatrix}$

7. Si illustrino le proprietà del gate CNOT e il suo utilizzo nel circuito quantistico che genera gli stati di Bell.

Il CNOT-gate è un tipo di *controlled U-gate* in cui l'operatore U è un Pauli-X gate.



La matrice del gate è: C(X) = $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

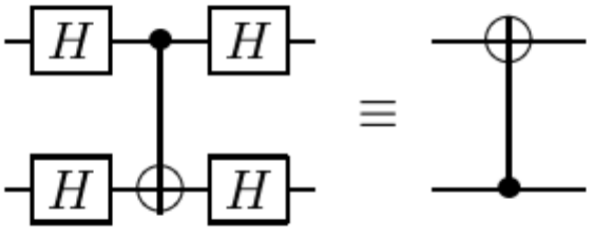
Definendo |c> = $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$e |t> =$\begin{pmatrix} t_1 \\ t_2 \end{pmatrix}$ allora:

C(x)|c > = $c_1t_1|00> + c_1t_2|01> + c_2t_2|10> + c_2t_1|11>$

<u>PROPRIETA:</u> CNOT Gate è *self-inverse*, ovvero: $C(X) = C(X)^{-1}$

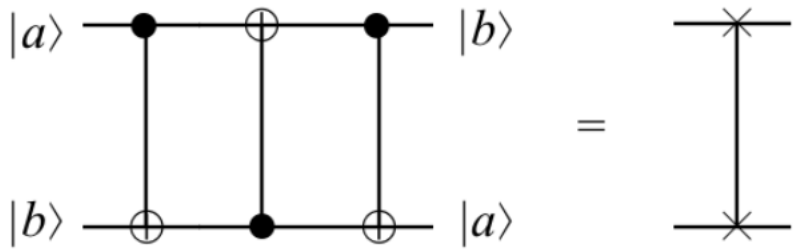
Per la seconda parte della domanda -> vedi domanda 3.

Un CNOT gate con 4 Hadamard gates posti prima e dopo il control ed il target costituiscono un CNOT gate con target e control invertiti.



8. Si mostri come il gate SWAP può essere implementato usando alcuni gate CNOT. Si ricavi di conseguenza la matrice del gate SWAP.

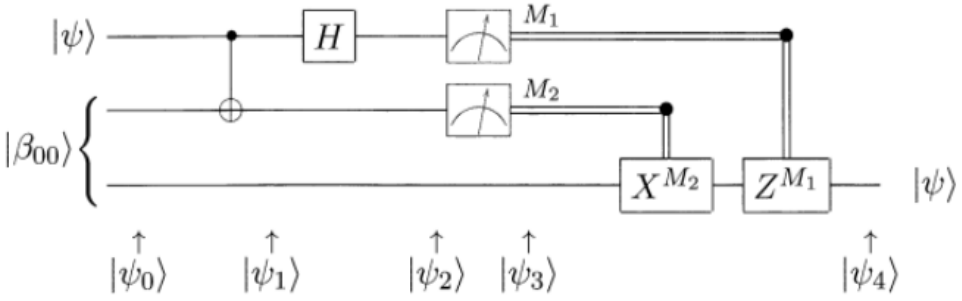
Lo SWAP-gate è un circuito per scambiare lo stato di due qubits $|a, b> \rightarrow |b, a>$. Può essere realizzato con 3 CNOT gates collegati in serie, con qubits target e control alternati.



La matrice unitaria è: $SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

9. Si illustri l'algoritmo del teletrasporto quantistico. Come viene utilizzato nei ripetitori quantistici?

Supponiamo che Alice vuole mandare un qubit state $|\psi>$ a Bob, Alice non conosce lo stato e può mandare solo informazioni classiche a Bob. La meccanica quantistica impedisce ad Alice di determinare lo stato quando ha solo una singola copia del qubit, la soluzione del problema è fornita da questo circuito:



Per il principio di *misurazione differita*, esiste anche una variante del circuito in cui le misurazioni sono poste alla fine.

I primi due qubit rappresentano il sistema di Alice, mentre il terzo quello di Bob.

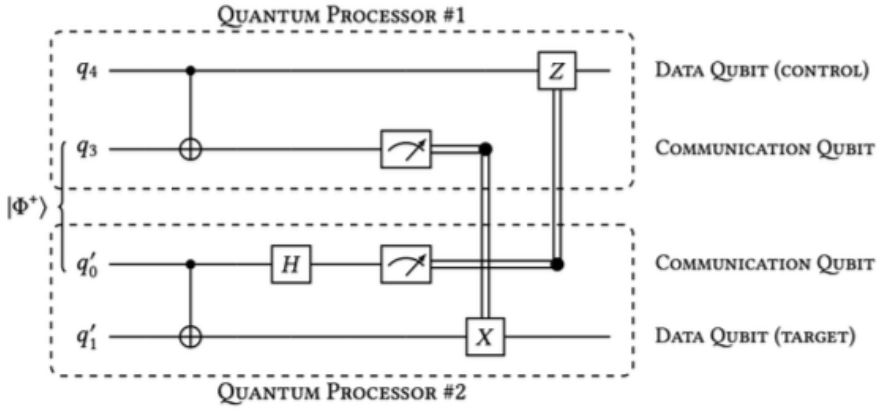
Gli stati del sistema sono:

$|\psi_0> = |\psi> |\beta_{00}> = \alpha|0> \frac{|00> + |11>}{\sqrt{2}} + \beta|1> \frac{|00> + |11>}{\sqrt{2}}$ -> stato iniziale globale

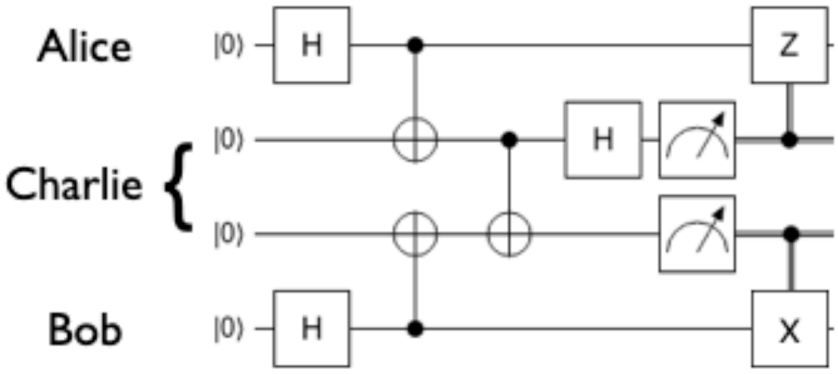
$|\psi_1 \geq = \frac{1}{\sqrt{2}}[\alpha|0> (|00> + |11>) + \beta|1> (|10> + |01>)]$ -> dopo CNOT

$$|\psi_2> = \frac{1}{2}[|00>(\alpha|0> + \beta|1>) + |01>(\alpha|1> + \beta|0>) + |10>(\alpha|0> - \beta|1>) + |11>(\alpha|1> - \beta|0>)]$$

Successivamente Alice misura il proprio qubit, in base al risultato della misurazione il qubit di Bob ha diversi stati post-misurazione (00,01,10,11) e li comunica mediante canali classici. Per ottenere $|\psi>$, Bob deve applicare $X^{M_2}Z^{M_1}$ al proprio qubit. Quando il teletrasporto è stato completato e solo il qubit di Bob è nello stato $|\psi>$, mentre il primo qubit di Alice è nello stato |0> oppure |1> non violando il principio di clonazione.



Nell'ambito del quantum internet viene utilizzato per realizzare l'*entanglement swapping* per muovere dati quantistici da un posto ad un altro.

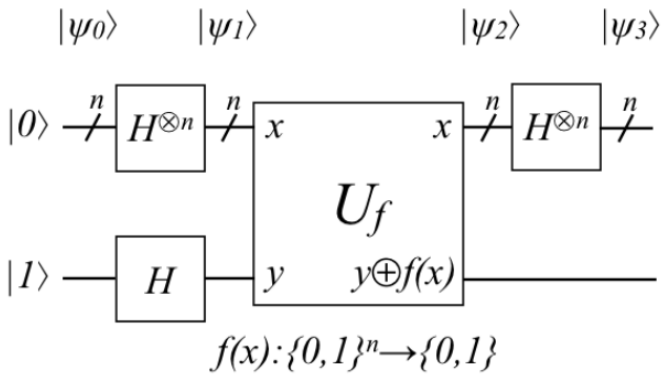


10. Si illustri l'algoritmo di Deutsch-Jozsa.

Il problema affrontato dall'algoritmo di Deutsch-Jozsa è il seguente:

Alisce sceglie x tra 0 e $2^n - 1$ e lo manda a Bob. Bob applica f(x) e riporta il risultato ad Alice. Alice sa che f(x) è bilanciato, cioè f(x) = 1 per la metà di tutti i possibili valori di x ed f(x) = 0 per l'altra metà. Trovare un algoritmo quantistico per decidere con una singola query, se Bob usa una f(x) costante oppure bilanciata.

Il circuito che rappresenta l'algoritmo è il seguente:



Alice usa n-qubit register per salvare la sua query ed un single-qubit register per salvare la riposta ricevuta da Bob. Lo stato iniziale preparato da Alice è:

$$|\psi_0> = |0>^{\otimes n} |1>$$

Applicando $|H>^{\otimes n}$ ad $|0>^{\otimes n}$ si ottiene

$$|\psi_1> = \sum_{x \in \{0,1\}^n} \frac{|x>}{\sqrt{2}^n} \left(\frac{|0> - |1>}{\sqrt{2}}\right)$$

L'output del gate U_f è:

$$|\psi_2> = \sum_{x \in 0,1^n} \frac{(-1)^{f(x)}|x>}{\sqrt{2}^n} \left(\frac{|0> - |1>}{\sqrt{2}}\right)$$

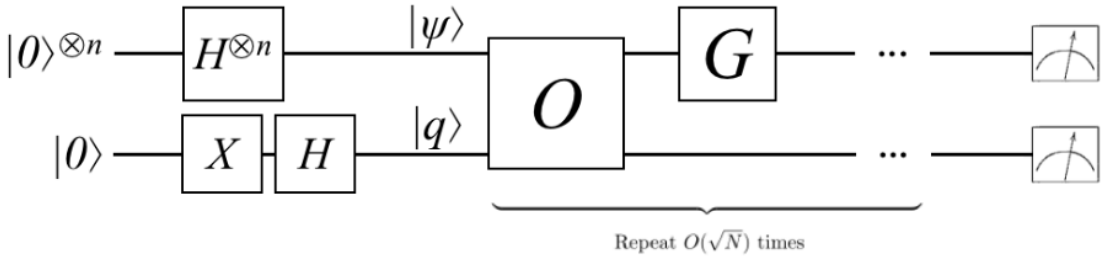
Dopo aver applicato il gate $|H>^{\otimes n}$ si ottiene:

$$|\psi_3> = \sum_z \sum_x \frac{(-1)^{x*z + f(x)}|z>}{2^n} \left(\frac{|0> - |1>}{\sqrt{2}}\right)$$

Lo stato $|z> = |0>^{\otimes n}$ ha ampiezza pari a $\sum_x \frac{(-1)^{f(x)}}{2^n}$
Se f(x) è <u>costante</u>, questa ampiezza è pari a +1 o -1, mentre tutte le altre ampiezze dovrebbero essere pari a 0; in questo caso Alice dovrebbe trovare tutti 0 quando osserva il suo query register. Se f(x) è <u>bilanciata</u> allora l'*interferenza distruttiva* porta l'ampiezza di |z> pari a 0. Quindi la misurazione produce un risultato diverso da 0 su almeno un qubit nel query register.

11. Si illustri l'algoritmo di Grover, disegnando anche il relativo circuito quantistico.

L'algoritmo di Grover serve per risolvere il problema di conoscere una soluzione valida in uno spazio di $N = 2^n$ soluzioni possibili, con $O(\sqrt{n})$ queries ad un oracolo per avere una probabilità vicino ad 1 di indovinare la soluzione giusta (normalmente la complessità sarebbe pari a O(n)).



Si usa un *quantum membership oracle O* in modo che:

$$|x> |q> \overset{O}{\rightarrow} |x> |q \oplus f(x)>$$

|q> è l'*ancilla state* (memoria del sistema) e f(x) è pari ad 1 se la soluzione è giusta.

G rappresenta il *Groover diffusion operator* che è definito come: $G = 2|\psi><\psi| - I$ con ψ che rappresenta la superposizione uniforme di tutti gli stati preparata applicando $|H>^{\otimes n}\ ad\ |0>^{\otimes n}$

O ha lo scopo di invertire l'ampiezza del target |x'> e tutti gli altri state non vengono modificati, G rende lo stato |x'> con ampiezza superiore alla media e diminuisce al di sotto di essa tutti gli altri stati. Se si ripete quanto fatto $O(\sqrt{n})$ volte, il target state |x'> viene amplificato su tutti gli altri stati nella superposition. GO può essere visto come una rotazione nello spazio bidimensionale attraversato dal vettore $|\psi>$ e dallo stato che rappresenta la soluzione; ripetere l'esecuzione di GO ruota lo state vector vicino ad |x'>.

12. Si illustri il circuito della QFT. In quale famoso algoritmo quantistico viene utilizzata e perché?

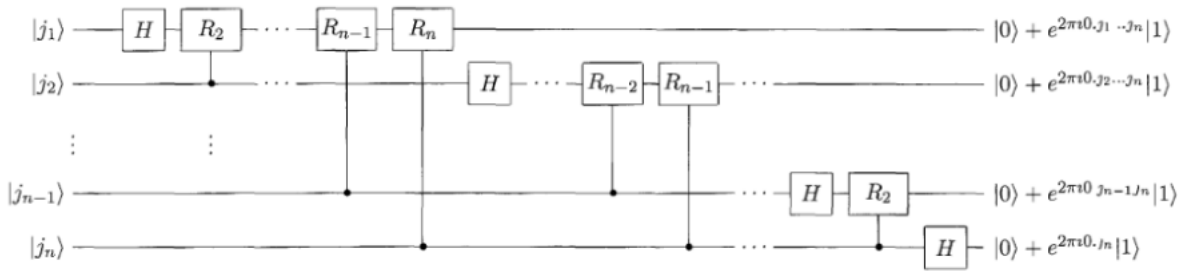
Il circuito della QFT permette di calcolare la *trasformata di Fourier Quantistica*

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$$

Che può essere riscritto come segue:

$$|j_1 j_2 \dots j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\dots(|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n)}|1\rangle)}{\sqrt{2^n}}$$

Il circuito che lo rappresenta è il seguente:



La versione QFT trasposta coniugata viene utilizzata nell'algoritmo di Shor per il calcolo della stima di φ espressa in t bits.

13. Si illustri il protocollo BB84 per la QKD.

Il protocollo BB84 è il primo protocollo sviluppato per il quantum key distribution, che consiste nell'usare la meccanica quantistica per rilevare la presenza o l'assenza di un intercettatore mentre Alice e Bob si scambiano stati quantistici con lo scopo di creare una chiave segreta condivisa.

Consiste in 7 passaggi:

1. Alice manda una serie di qubits a Bob che codificano i bits mediante le loro basi.
2. Bob misura ogni qubit che riceve usando una base scelta casualmente
3. Alice e Bob tengono un paio di stringhe di bit chiamate *raw pair key*
4. SIFTING: Bob ed Alice scambiano la sequenza delle basi che scelgono. Per ogni paio di bit $(x_i y_i)$, se la base corrispondente corrisponde allora la coppia viene mantenuta (altrimenti viene scartata)
5. PARAMETER ESTIMATION: Alice e Bob confrontano alcuni set di bit scelti a caso, al fine di ottenere un'ipotesi per il tasso di errore, cioè la frazione di posizioni in cui le loro stringhe di bit non corrispondono. Se il tasso di errore

è troppo grande allora il protocollo viene abortito, altrimenti la parte rimanente delle chiavi viene salvata con $(x'_o, \ldots, x'_m;\ y'_o, \ldots, y'_m)$

6. INFORMATION RECONCILIATION: Alice invia alcune informazioni di correzione degli errori a Bob, permettendo a Bob di calcolare un'ipotesi per $(x'_o, \ldots, x'_m)$.
7. PRIVACY AMPLIFICATION: Alice e Bob trasformano $(x'_o, \ldots, x'_m)$ in una chiave più corta e sicura utilizzano procedure di Hash.

Possibili domande (mai uscite negli esami)

1. **Parlare della Trace distance.**

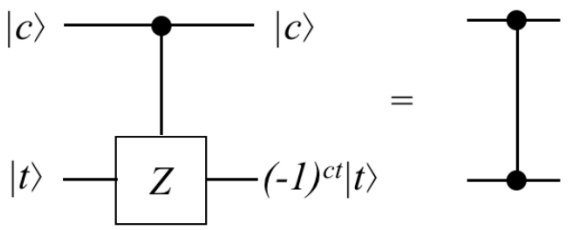
   È una misura della distanza che permette di stabilire quanto due quantum state siano vicini tra loro. La *trace distance* tra due operatori densità ρ, σ è la traccia normale della loro differenza:

   $$||\rho - \sigma||_1 = tr\sqrt{(\rho - \sigma)^T(\rho - \sigma)}$$

   Vale 0 se i due quantum state sono uguali, ovvero se nessuna misurazione distingue $\rho\ da\ \sigma$.

   È massima se i due quantum state hanno supporto sul sottospazio ortogonale, ovvero se esiste una misurazione che distingue perfettamente i due stati.

2. **Illustrare il Controlled phase gate.**



   La sua matrice unitaria è: $C(Z) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$, la sua azione è:

   $|c, t> \rightarrow (-1)^{ct}|c, t>$

   È possibile realizzare un CNOT mediante un Controlled-Phase Gate e due Hadamard gates

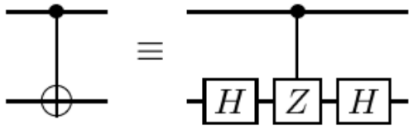


Figure 11: CNOT with a Controlled-Phase gate and two Hadamard gates.

3. **Parlare dei processi quantistici.**

   I processi quantistici possono catturare processi fisici come la preparazione dello stato, gli effetti del rumore oppure l'evoluzione unitaria, la misurazione etc. Un quantum channel è visto come un processo quantistico pipeline che trasporta informazione quantistica. I processi quantistici sono rappresentati come operatori di Kraus $\varepsilon(\rho) = \sum_i k_i \rho k_i^\dagger$. ε è l'azione del processo sullo stato ρ.
   La probabilità di ogni Kraus operator è $p_i = tr(K_i \rho K_i^\dagger)$
   I processi sono *trace preserving*, ovvero tr($\varepsilon(\rho)) = 1$, ed inoltre è possibile applicare la composizione di processi multipli $\varepsilon(\rho_1 + \rho_2) = \varepsilon(\rho_1) + \varepsilon(\rho_2)$

4. **Parlare del quantum decoherence e dephasing.**

   Il quantum decoherence è un evoluzione non unitaria di un sistema quantistico aperto e non isolato, si può pensarla come un insieme di evoluzioni unitarie, a cui ogni membro dell'insieme viene assegnata una probabilità. È il processo irreversibile per cui uno stato puro diventa mixed.
   Il dephasing channel crea un mix di uno stato di input con sé stesso phase-flipped.
   Il dephasing influisce su tutte le attuali architetture di quantum computing, utilizzano la Kraus representation può essere visto come: $\varepsilon^{dephasing}(\rho) = (1-p)\rho + pZ\rho Z$

   Con p che è la probabilità, ρ è lo stato di un singolo qubit e z è l'operatore Pauli Phase-Flip.

5. **Parlare del gate Measurement e del circuito di misurazione dei Bell state.**

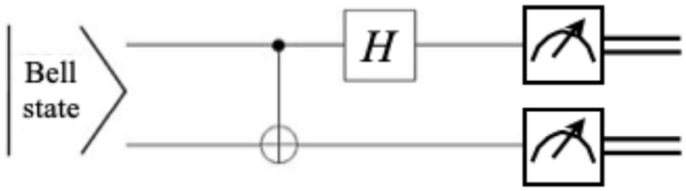
   La misurazione può essere vista come un gate che converte uno stato $|\psi> = \alpha|0> + \beta|1>$ in un bit classico M che vale 0 con probabilità alpha^2 oppure 1 con probabilità beta^2.

   Due principi fondamentali sulla misurazione sono: *la misurazione differita*, che afferma che la misurazione situata nel mezzo di un circuito può essere spostata alla fine del circuito senza incidere sul risultato ottenuto da essa.
   Il *principio di misurazione implicita* afferma che i qubits che non sono stati misurati alla fine di un circuito quantistico possono essere considerati misurati senza perdita di generalità.

   Per eseguire una misurazione in altre basi $\{|x>, |x^\perp>\}$ diverse da quella computazionale, bisogna applicare un operatore unitario che trasformi la base in una base computazionale e applicarlo prima di misurare tale base. L'operatore sarà del tipo:

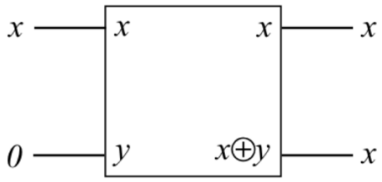
$$U = |0\rangle\langle x| + |1\rangle\langle x^\perp|.$$

Il circuito di misurazione dei Bell State è fondamentale nell'ambito del quantum network:



6. Illustrare il circuito per clonare un quantum state.

Per il teorema della non-clonazione sappiamo che non è possibile copiare uno stato sconosciuto. Nel caso sapessimo che lo stato appartiene ad una base ortonormale (Es. |0>, |1>), il seguente circuito è valido:



7. Illustrare l'Uncomputation Trick.

Un algoritmo che calcola una f(x) è *clean* se quando eseguito sullo stato iniziale:

$|x\rangle|0\rangle^{\otimes m}|0\rangle$

Si ottiene: $|x\rangle|0\rangle^{\otimes m}|f(x)\rangle$

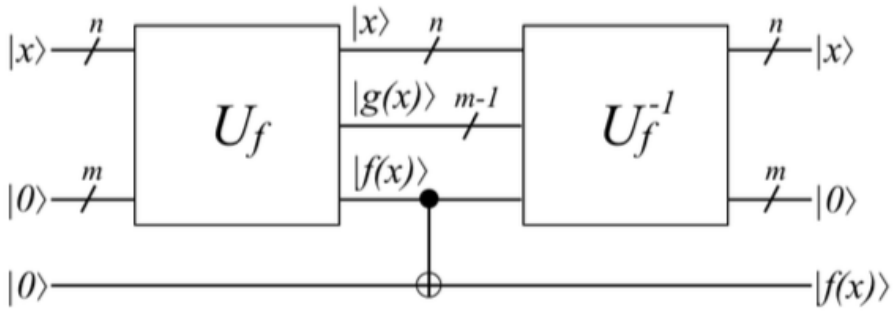
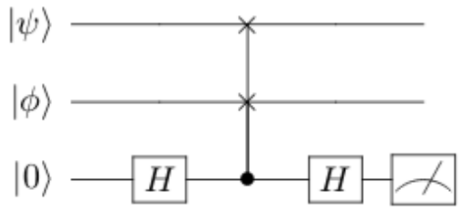


Figure 19: Quantum circuit that computes $f(x)$ in a clean fashion, i.e., uncomputing garbage on ancilla qubits.

Nel circuito in figura, la memoria di lavoro è stata pulita ma il risultato del calcolo viene memorizzato in modo sicuro nell'ultimo qubit.

8. Illustrare il circuito controlled swap test

Il circuito quantistico mostrato consente il test di swap controllato: se dalla misurazione finale si osserva uno 0, allora |ψ⟩ e |ϕ⟩ sono vicini l'uno all'altro, mentre osservare un 1 indica che sono molto distanti. N.B gli stati in input sono sconosciuti



9. Descrivere cos'è il quantum interference e cosa sono i quantum oracles.

Consideriamo lo stato |0>, applicando due volte il gate rad(NOT) otteniamo lo stato |1>. Nonostante ci sono due "percorsi" che producano come risultato |0>, essi hanno ampiezza con segni opposti (interferenza distruttiva); entrambi i cammini che portano ad |1> hanno ampiezza positiva (interferenza costruttiva).
Il concetto d'interferenza è il core della meccanica quantistica e del quantum computing, si cerca di ottenere percorsi con ampiezze positive e negative per le risposte sbagliate mentre percorsi con ampiezze solo positive per le risposte giuste ai nostri problemi.
Un *quantum oracle* è un circuito black box che agisce su un input state e produce un output state secondo alcune funzioni f. La *query complexity* indica il numero di volte che bisogna chiamare l'oracolo all'interno dell'algoritmo più noto per risolvere il problema. Il *quantum membership oracle* è una trasformazione unitaria definita come: U_f: $|x, q> \rightarrow |x, q \oplus f(x)>$ con $f(x) \in \{0,1\}, q \in \{0,1\},\ x \in \{0,1\}^n$
Supponiamo che ci sia uno spazio di soluzioni N= 2^n soluzioni, un intero x rappresenta una soluzione al problema di ricerca se f(x)=1. Prepariamo |x>|0>, applichiamo l'oracolo U_f e si vede se l'ancilla state |q> è stato cambiato ad |1>, se Si allora x è la soluzione.

10. Descrivere il protocollo E91.

E91 è un protocollo per il quantum key distillation, che permette a due nodi di trasformare auto-copie condivise in una chiave comune segreta. Consiste in 4 passaggi:

1. Un PR PNR Generator produce un flusso di coppie di fotoni, per ogni coppia Alice e Bob ricevono un fotone e lo misurano usando una base scelta casualmente.
2. Usando un canale pubblico autenticato, Bob ed Alice scambiano le sequenze delle basi che hanno scelto.
3. Vengono generati due gruppi di bit: il primo contiene i bit ottenuti misurando nella stessa base, il secondo tutti gli altri.
4. Alice e Bob controllano la violazione della disuguaglianza CHSH, in caso di nessuna violazione (== uno dei due stati non è entangle) significa che c'è stato un eavesdropping -> Abort! Altrimenti usano il primo gruppo di bit come chiave condivisa.